

REMARKS

Claims 1-15 are pending. These claims have been amended to place them in a form which comports with established U.S. claim practice. Also, the specification has been amended to include section headers, and a new abstract has been provided.

It is respectfully submitted that the application is in condition for allowance. Favorable consideration and prompt allowance of the application is respectfully requested.

Should the Examiner believe that further amendments are necessary to place the application in condition for allowance, or if the Examiner believes that a personal interview would be advantageous in order to more expeditiously resolve any remaining issues, the Examiner is invited to contact Applicant's undersigned attorney at the telephone number listed below.

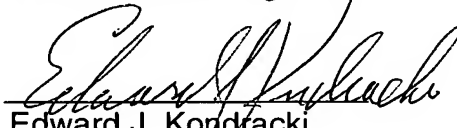
To the extent necessary, Applicant petitions for an extension of time under 37 CFR § 1.136. Please charge any shortage in fees due in connection with this application, including extension of time fees, to Deposit Account No. 50-1165 (Attorney Docket No. T2146-907683) and credit any excess fees to the same Deposit Account.

Respectfully submitted,

Miles & Stockbridge P.C.

Date: January 9, 2002

By:


Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone No: (703) 610-8641
Facsimile No: (703) 610-8686

Marked-Up Version of the Amended Claims

1 1. (Amended) [Method] A method for authenticating a portable object [(7)
2 comprising] including information processing means [(8)] and information storage
3 means [(9, 10)], the information storage means containing at least one code [(i)]
4 defining [operations] operation steps capable of being executed by the portable
5 object, as well as a one-way function, [characterized in that it comprises the step that
6 consists of] comprising sending the portable object an order [(31, 32i-34i, 35, 36) so
7 that the latter executes a] for executing a calculation of a result by applying to said
8 one-way function at least part of said code [(i)], [this] and using said result [being
9 used] to decide whether or not the portable object is authentic.

1 2. (Amended) [Method] A method according to claim 1, wherein said
2 result enters into the implementation of a [given] predetermined operation, [this] said
3 operation being performed successfully only when the portable object [(7)] is
4 authentic.

1 3. (Amended) [Method] A method according to claim 2, wherein said
2 [given] predetermined operation comprises a decryption operation, said result
3 making it possible to produce an associated decryption key.

1 4. (Amended) [Method] A method according to claim 1, wherein said part
2 of said code [part (i)] used in the calculation, comprises a machine code [part].

5. (Amended) [Method] A method according to claim 1, wherein the portable object [(7)] contains a [so-called "real"] real code defining operations designed to be executed by the portable object, and a [so-called "dummy"] dummy code defining operations not designed to be executed by the portable object, said code [part] used in the calculation of a result comprising a dummy code [part].

6. (Amended) [Method] A method according to claim 1, [wherein said order (31, 32i-34i, 35, 36) is sent] further comprising repeatedly sending said order to the portable object [repeatedly] during its life, prior to [the] execution by the [latter] portable object of said [operations] operation steps.

7. (Amended) [Method] A method according to claim 1, wherein said code [part (i)] used in the calculation is defined by a start address [(32i)] and an end address [(33i)] in the information storage means, and further including the step of sending said start and end addresses [being sent] to the portable object.

8. (Amended) [Method] A method according to claim 1, wherein said code [(i)] comprises a set of binary words, said code [part] used in the calculation being defined by a subset of said binary words comprising [the] binary words distributed in the information storage means at a determined pitch [(34i)], said pitch being sent to the portable object.

9. (Amended) [Method] A method for having a portable object [(7)] execute a sensitive operation, the portable object comprising information processing means [(8)] and information storage means [(9, 10)], comprising: storing in the

information storage means [containing] at least one code [(i)] defining operations capable of being executed by the portable object, as well as a one-way function, and [characterized in that it comprises the step that consists of] sending the portable object an order [(31, 32i-34i, 35, 36)] so that the [latter] portable object executes a calculation of a result by applying to said one-way function at least part of said code [(i)], said result entering into the implementation of said sensitive operation, [this] said operation being performed successfully only when the portable object [(7)] is authentic.

10. (Amended) [Method] A method according to claim 9, wherein [said] the code part [(i)] used in the calculation comprises a machine code [part].

11. (Amended) [Method] A method according to claim 9, wherein the portable object contains a [so-called "reel"] real code defining operations designed to be executed by the portable object, and a [so-called "dummy"] dummy code defining operations not designed to be executed by the portable object, said code part used in the calculation comprising a dummy code [part].

12. (Amended) [Portable] A portable object, comprising: information processing means, [(8) and] information storage means [(9, 10)], the information storage means containing at least one code [(i)] defining operations capable of being executed by the portable object, as well as a one-way function, [characterized in that it comprises] and means for executing a calculation of a result by applying to said one-way function at least part of said code.

1 13. (Amended) [Portable] A portable object according to claim 12,
2 wherein said code part [(i)] used in the calculation comprises a machine code [part].

1 14. (Amended) [Device (1)] A device comprising: information processing
2 means, [(2) and] information storage means [(3, 4) and] , said information processing
3 means designed to communicate with a portable object [(7)] in order to authenticate
4 the [latter] portable object, the portable object comprising: information processing
5 means, [(8) and] information storage means [(9, 10)], the information storage means
6 of the portable object containing at least one code [(i)] defining operations capable of
7 being executed by the portable object, as well as a one-way function, [characterized
8 in that it comprises] and means for sending the portable object an order [(31, 32i-34i,
9 35, 36)] so that the [latter] portable object executes a calculation of a result by
10 applying to said one-way function at least part of said code [(i)] of the portable object.

1 15. (Amended) [Device] A device according to claim 14, wherein said
2 code part [(i)] used in the calculation comprises a machine code [part].